

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-073309

(43)Date of publication of application : 16.03.1999

(51)Int.Cl.

G06F 9/06

(21)Application number : 09-231381

(71)Applicant : NEC CORP

(22)Date of filing : 27.08.1997

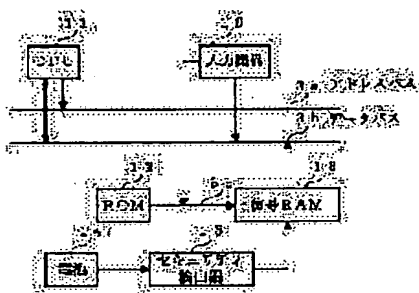
(72)Inventor : WATANABE TAKASHI

(54) INSTRUCTION CODE PROTECTION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To attain a simple instruction code protection system capable of preventing an instruction code stored in an ROM from being easily analyzed.

SOLUTION: A CPU 11 outputs the address of an instruction code or data to be accessed to an address bus 3a and an ROM 12 stores a ciphered instruction code outputted from the CPU 11. A decoding RAM 13 inputs the ciphered instruction code outputted from the ROM 12 as an address and stores conversion data to be decoded and a decoded instruction code is sent to the CPU 11 through a data bus 3b. A battery 14 supplies power for storing the conversion data stored in the RAM 13. A security detector 15 detects action intending the analysis of the instruction code and stops power supply from the battery 14 to the RAM 13. An input mechanism 16 writes the contents of the RAM 13 from the external independently of the operation of the CPU 11.



LEGAL STATUS

[Date of request for examination] 27.08.1997

[Date of sending the examiner's decision of rejection] 10.07.2001

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

This Page Blank (uspto)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-73309

(43) 公開日 平成11年(1999) 3月16日

(51) Int.Cl.⁶

G 0 6 F 9/06

識別記号

5 5 0

F I

G 0 6 F 9/06

5 5 0 B

審査請求 有 請求項の数 4 O L (全 4 頁)

(21) 出願番号

特願平9-231381

(22) 出願日

平成9年(1997) 8月27日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 渡邊 貴志

東京都港区芝五丁目7番1号 日本電気株式会社内

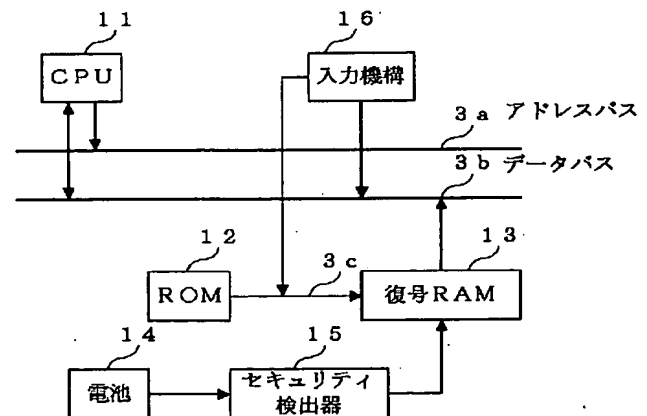
(74) 代理人 弁理士 京本 直樹 (外2名)

(54) 【発明の名称】 命令コード保護システム

(57) 【要約】

【課題】 ROMに格納されている命令コードを容易に解析されないための簡便な命令コード保護システムを実現する。

【解決手段】 CPU 11は、アドレスバス 3 a にアクセスすべき命令コードやデータのアドレスを出力し、ROM 12は暗号化されたCPU 11の命令コードを格納する。復号RAM 13はROM 12の出力した暗号化された命令コードをアドレス入力とし、復号化するための変換データを記憶し、復号された命令コードはデータバス 3 b を通してCPU 11へ送出される。電池 14は復号RAM 13に記憶されている変換データを保持するための電力を供給する。セキュリティ検出器 15は命令コードの解析を意図した行為を検出して電池 14から復号RAM 13への電力供給を停止する。入力機構 16はCPU 11の動作に無関係に復号RAM 13の内容を外から書き込む。



【特許請求の範囲】

【請求項1】 (a) 暗号化された命令コードを格納するリードオンリーメモリと、(b) 前記リードオンリーメモリからの暗号化された命令コードを復号しデータバスに出力するための変換データを記憶する揮発性の復号ランダムアクセスメモリと、(c) 前記復号ランダムアクセスメモリの記憶内容を保持するための電力を供給する電池と、(d) 命令コードの解析を意図した筐体の分解を含む操作を検出し前記電池から前記復号ランダムアクセスメモリに供給される電力を切断するセキュリティ検出器と、(e) 前記復号ランダムアクセスメモリに記憶される変換データを外部より書き込むための入力機構と、を備えることを特徴とする命令コード保護システム。

【請求項2】 前記リードオンリーメモリに対し、アドレスバスを介してアドレスを与え、前記復号ランダムアクセスメモリからの復号された命令コードを前記データバスを介して取り込むCPUを備えることを特徴とする請求項1記載の命令コード保護システム。

【請求項3】 前記入力機構が、前記復号ランダムアクセスメモリに対し前記アドレスバスを介してアドレスを与え、前記データバスを介して前記変換データを書き込むことを特徴とする請求項2記載の命令コード保護システム。

【請求項4】 前記リードオンリーメモリおよび前記復号ランダムアクセスメモリを1チップで構成することを特徴とする請求項1、2または3記載の命令コード保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、保護システムに関し、特に、コンピュータのプログラムに使用される命令コードを解析から保護するための命令コードシステムに関する。

【0002】

【従来の技術】従来の技術としては、たとえば、「特開平2-155034号公報」記載の「セキュリティ機能付き計算機」がある。この技術は、記憶装置上の機械語命令およびデータを中央処理装置に取り込んで解釈しながら実行する計算機であって、前記中央処理装置内に設けられる鍵格納用の格納手段と、この格納手段に格納されている鍵を用いて前記記憶装置から暗号化された機械語命令およびデータを読み出して中央処理装置で使用可能な機械語命令およびデータに復元する暗号復元手段と、前記格納手段に格納されている鍵を用いて前記記憶装置に格納されるデータを暗号化して前記記憶装置に格納する暗号化手段とを備える計算機である。

【0003】

【発明が解決しようとする課題】上述した従来の技術の問題点は、暗号化・復号部と記憶装置とを別々に解析し

ても命令コードやデータの秘匿性は保たれるが、暗号化・復号部と記憶装置とを総合して解析すると、記憶装置内の命令コードやデータを解読することができ、セキュリティが保証されないことである。その理由は、暗号化・復号部を中央処理装置内に持つからである。

【0004】本発明の目的は、装置全体を解析しても、命令コードの秘匿性が維持がされセキュリティが保証される命令コード保護システムを実現することである。

【0005】

【課題を解決するための手段】本発明の第1の命令コード保護システムは、(a) 暗号化された命令コードを格納するリードオンリーメモリと、(b) 前記リードオンリーメモリからの暗号化された命令コードを復号しデータバスに出力するための変換データを記憶する揮発性の復号ランダムアクセスメモリと、(c) 前記復号ランダムアクセスメモリの記憶内容を保持するための電力を供給する電池と、(d) 命令コードの解析を意図した筐体の分解を含む操作を検出し前記電池から前記復号ランダムアクセスメモリに供給される電力を切断するセキュリティ検出器と、(e) 前記復号ランダムアクセスメモリに記憶される変換データを外部より書き込むための入力機構と、を備える。

【0006】本発明の第2の命令コード保護システムは、前記第1の命令コード保護システムであって、前記前記リードオンリーメモリに対し、アドレスバスを介してアドレスを与え、前記復号ランダムアクセスメモリからの復号された命令コードを前記データバスを介して取り込むCPUを備える。

【0007】本発明の第3の命令コード保護システムは、前記第2の命令コード保護システムであって、前記入力機構が、前記復号ランダムアクセスメモリに対し前記アドレスバスを介してアドレスを与え、前記データバスを介して前記変換データを書き込む。

【0008】本発明の第4の命令コード保護システムは、前記第1、2または3の命令コード保護システムであって、前記リードオンリーメモリおよび前記復号ランダムアクセスメモリを1チップで構成する。

【0009】

【発明の実施の形態】次に、本発明の実施の形態について図1を参照して詳細に説明する。図1は、本発明の実施の形態を示すブロック図である。

【0010】図1を参照すると、本発明の命令コード保護システムは、アドレスバス3aにアクセスすべき命令コードやデータのアドレスを出力し、データバス3bを用い命令コードやデータの入出力を行うCPU11と、暗号化されたCPU11の命令コードを格納するリードオンリーメモリであるROM12と、ROM12の出力した暗号化された命令コードをアドレス入力とし、復号化するための変換データを記憶し、復号された命令コードをデータバス3bを通してCPU11へ送出するラン

ダムアクセスメモリである復号RAM13と、復号RAM13に記憶されている変換データを保持するための電力を供給する電池14と、命令コードの解析を意図した筐体の分解等の行為を検出して電池14から復号RAM13への電力供給を停止する機能を持つセキュリティ検出器15と、CPU11の動作に無関係に復号RAM13の内容を外部から書き込むための入力機構16とから構成される。

【0011】次に、上記本発明の命令コード保護システムの動作に関して図1を参照して説明する。CPU11は命令コードを読み出す際にアドレスバス3aにアクセスするアドレスを出力する。このアドレスは命令コードが暗号化されて格納されているROM12に与えられ、暗号化された命令コードがデータ線3cに出力される。

【0012】暗号化された命令コードはデータ線3c経由で復号RAM13へアドレスとして供給される。復号RAM13には暗号化されたアドレスパターンからデータを復号するための復号データがあらかじめ格納されている。データ線3cによって供給された暗号化された命令コードは復号RAM13の復号データによって復号化されデータバス3b経由でCPU11に供給される。以上の手順でCPU11は正しい命令コードを得ることができる。

【0013】復号RAM13内の復号データは電池14の電力によって保持されているが、セキュリティ検出器15が命令コードの解析を意図した筐体の分解等の行為を検出した場合には、電池14から復号RAM13への電力供給が停止され、これにともない復号RAM13内の復号データは破壊される。以後、復号RAM13は復号機能を失い、またROM12は暗号化されているため命令コードを容易に解析することができない状態となる。

【0014】また、入力機構16を用いて復号RAM13へ復号データを書き込むことができる。

【0015】次に本発明の実施の形態の実施例に関して図2を参照して詳細に説明する。図2は本発明の実施例を示すブロック図である。語長8ビットのCPU21は、アドレスバス3aにアクセスすべき命令コードやデータのアドレスを出力し、8ビットデータバス3bを用い命令コードやデータの入出力を行う。

【0016】ROM22はデータビット位置を組み替えて暗号化されたCPU21の命令コードを格納している。

【0017】復号RAM23はROM22の出力した暗号化された命令コードをアドレス入力とし、正しいデータビット位置に組み替えて復号化するための変換データを記憶している。また、復号された命令コードは8ビットデータバス3bを通してCPU21へ伝達される。復号RAM23は、「2の8乗」=256【バイト】の容量を有すればよい。

【0018】電池24は復号RAM23に記憶されている変換データを保持するための電力を供給する。

【0019】筐体分解検出センサ25は命令コードの解析を意図した筐体の分解を検出するセンサ機能を有し、筐体の分解を検出した場合に電池24から復号RAM23への電力供給を停止する機能を持つ。

【0020】入力機構26はCPU21の動作に無関係に復号RAM23の内容を外部から書き込むための機構である。

【0021】次に上記本発明の実施例の動作について図2を参照して説明する。CPU21は命令コードを読み出す際にアドレスバス3aにアクセスするアドレスを出力する。このアドレスは命令コードが暗号化されて格納されているROM22に与えられ、暗号化された命令コードがデータ線3cに出力される。

【0022】暗号化された命令コードはデータ線3c経由で復号RAM23へアドレスとして供給される。復号RAM23には供給された暗号化されたアドレスパターンからデータを復号するための復号データがあらかじめ入力機構26を用いて格納されている。データ線3cによって供給された暗号化された命令コードは復号RAM23の復号データによって復号化されデータバス3b経由でCPU21に供給される。以上の手順でCPU21は正しい命令コードを得ることができる。

【0023】復号RAM23内の復号データは電池24の電力によって保持されているが、筐体分解検出センサ25が命令コードの解析を意図した筐体の分解を検出した場合には、電池24から復号RAM23への電力供給が停止され、これにともない復号RAM23内の復号データは破壊される。以後、復号RAM23は復号機能を失い、またROM22は暗号化されているため命令コードを容易に解析することができない状態となる。また、入力機構26を用いて復号RAM23へ復号データを書き込むことができる。

【0024】次に、筐体分解検出センサ25の機能の詳細について図3を参照して説明する。図3は、筐体分解検出センサ25の機能を示すブロック図である。筐体31は、1面が開いた立方体あるいは直方体であり、その開口面は側板32とネジ34により密閉される。筐体分解検出センサ25（マイクロスイッチ）は、筐体31内に実装され、開口面に向かって接触感知センサ33が突起している。また、信号線4aは、電池24に接続され、信号線4bは、複合RAM23に接続されている。

【0025】側板32が、ネジ34により筐体31に固定された状態では、接触感知センサ33により信号線4aと信号線4bとが接続された状態になり、電池24から複合RAM23に電源が供給される。筐体を分解するために、ネジ34をゆるめると、接触感知センサ33により信号線4aと信号線4bとが断続された状態になり、電池24からの電源は、複合RAM23に供給され

なくなり、複合RAM23の内容は破壊される。

【0026】また、ROM22および復号RAM23を1チップで構成し、実装効率を向上させることができる。

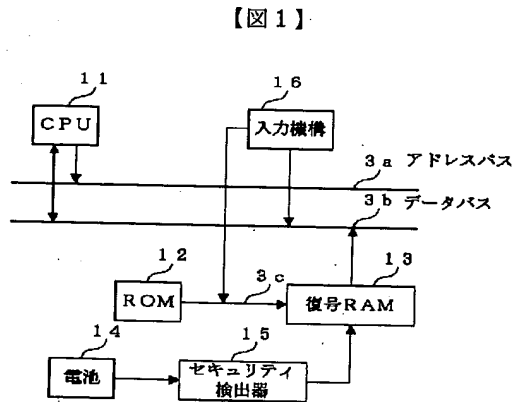
【0027】

【発明の効果】本発明の第1の効果は、装置全体を解析しても、命令コードの秘匿性が維持がされセキュリティが保証される命令コード保護システムを実現できることである。その理由は、復号手段を容易に復号手段を破壊することができる揮発性の復号RAMに格納し、命令コード自体は暗号化してROMに格納することにより、ROMを単独で解析しても容易に復号された命令コードを読み取ることができず、命令コードが保護されるからである。

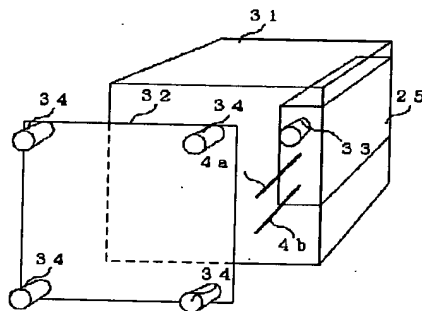
【0028】第2の効果は、実装効率を向上させることが可能となることである。その理由は、ROMおよび復号RAMを1チップで構成するからである。

【図面の簡単な説明】

【図1】本発明の実施の形態を示すブロック図である。



【図3】



【図2】本発明の実施例を示すブロック図である。

【図3】図2の筐体分解検出センサの機能を示すブロック図である。

【符号の説明】

- 11、21 CPU
- 12、22 ROM
- 13、23 復号RAM
- 14、24 電池
- 15 セキュリティ検出器
- 16、26 入力機構
- 25 筐体分解検出センサ
- 3a アドレスバス
- 3b データバス
- 3c データ線
- 31 筐体
- 32 側板
- 33 接触感知センサ
- 34 ネジ
- 4a、4b 信号線

【図2】

